Amenazas de seguridad informática y el manejo de datos en las empresas

Castro Páez, Ana Rocío.
anitarcp@gmail.com
Universidad Piloto de Colombia

Resumen—El manejo adecuado de la seguridad De la información en las empresas debe tener un manejo adecuado, al masificarse taques en busca de aprovechamiento de vulnerabilidades latentes pata robar y/o manipular información con fines indebidos.

De esta manera se debe concientizar al personal que hace parte de la empresa, directa e indirectamente, pues la vulnerabilidad más importante es aprovechar el desconocimiento o pensamiento y forma de actuar del talento humano.

El tratamiento de los datos personales es un tema importante a tratar, pues al ser suministrados, estos pueden llegar a ser manipulados de forma indebida. Por lo cual el estado Colombiano crea la ley estatutaria 1581 De 2012, para regular la protección de los datos personales.

Abstract—The proper management of information security in companies must have adequate management, the massively taques looking for utilization of latent vulnerabilities leg steal and / or manipulate information for improper purposes.

Thus staff should be made aware that is part of the company directly and indirectly, as the most important vulnerability is to exploit the ignorance or thought and modus operandi of human talent.

The processing of personal data is an important issue to address, for being supplied, these can become handled improperly. Therefore the Colombian state statutory law creates 1581, 2012 to regulate the protection of personal data.

Índice de Términos—Amenazas cibernéticas, concientización de talento humano, datos personales, Seguridad informática.

I. INTRODUCCIÓN

Gracias al auge de la tecnología hoy en día se establece el registro e intercambio de información de forma fácil, sin pensar en las consecuencias que esto puede acarrear, lo que ha hecho que se deba definir una serie de medidas, que controlen el manejo y administración de los datos que son suministrados y almacenados en bases de datos de entidades públicas y privadas.

Para las empresas es por lo tanto muy importante la forma como se implementa y se concientizan a los empleados sobre los riesgos que conlleva no usar los datos de forma óptima, así como los tipos de ataques que existen para el robo y uso indebido de la información que ellos manejan a diario.

Se deben definir una serie de controles a los procesos y a las tecnologías usadas, como por ejemplo el uso de los dispositivos móviles, los cuales son utilizados para manipular información laboral, siendo este un flanco de ataque cada vez más en la mira de personas inescrupulosas, quienes buscan robar y explotar la información de la empresa.

Se ha deliberado en búsqueda de métodos que hagan que el manejo de los datos, incluidos los que son de tipo personal para que sean controlados y no

pueda ser utilizado con fines indebidos y con consecuencias nefastas, como es el caso de los datos personales, que se definen como los que pertenecen a una persona, que sólo le compete a ella; de tal forma que pueden llegar a ser usados como método discriminatorio, es que aquella información que puede definirse como delicada, por lo tanto se debe manejar con precaución y manteniendo la privacidad, como parte fundamental e indispensable.

II. AMENAZAS EN LAS EMPRESAS

A. Ingeniería social

Es un tipo de ataque activo que busca mediante una serie de preguntas a personas, conocer información clave para descubrir los datos que son usados como objetivo para conseguir un tipo de lucro económico y/o de conocimiento que pertenece a un individuo u organización.

Hay un recurso inseguro que almacena información muy sensible: la mente humana. Ya sea por olvido o por el reto que implica asegurar la información dentro de las cabezas de sus empleados, las organizaciones no le prestan mucha atención a este aspecto. La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo. [1]

La Ingeniería Social se sustenta en un sencillo principio: "el usuario es el eslabón más débil". Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla [2]

B. Phishing

Este tipo de ataque de suplantación de identidad que busca a través de ingeniería social obtener información de la compañía, aprovechando, en la mayoría de los casos la falta de conocimiento por parte de los usuarios sobre los métodos de ingeniería social y las consecuencias que puede conllevar el manejo de la información sin precauciones de seguridad.

Se ha determinado que este tipo de ataques a las empresas se ejecutan de acuerdo a su naturaleza, "pues se orienta de la siguiente forma: Bancos: 40,4 % comercio electrónico: 16.6% Transferencias de dinero: 19.6% Redes sociales y correo: 12.4% Otros: 11.0%." [3]

C. Amenazas a dispositivos móviles

Hoy en día se hace uso de los dispositivos móviles como herramienta de trabajo, realizar operaciones transaccionales, estar en contacto con las redes sociales, entre otros, lo cual hace que estén en la mira de personas inescrupulosas que buscan aprovechar las vulnerabilidades para encontrar y explotar información valiosa, ya sea de tipo personal como laboral.

Además cuando los equipos se salen del perímetro seguro de la organización y cuando vuelvan a ingresar pueden traer consigo algún tipo de código malicioso. Si se usa el móvil para acceder información confidencial, hay que tener medidas adecuadas para que proteger los datos. [4]

Por lo tanto en las organizaciones se implantan una serie de medidas a los dispositivos móviles en los cuales se van a manejar correo electrónico de la entidad o información propia de la organización.

De tal manera que se instalan certificados de seguridad y se establece una conexión a servidores que tienen la propiedad para monitorear el

comportamiento de los cambios que pueda tener el dispositivo móvil, al igual que eliminar los datos del dispositivo, ya sea de trabajo o en su totalidad, en caso de pérdida o robo.

D. Ataque a sistemas de control Industrial

En los últimos tiempos los Sistemas de control industrial están conectados a internet, de tal forma que es un tema delicado pues pueden ser sistemas que controlan servicios públicos o privados.

Se han detectado casos en los cuales a través de ataques cibernéticos ha provocado interrupción de servicio celular y de ataques constantes a un servicio público nacional de electricidad.

E. Ciberespionaje

También llamado ciberguerra o ciberterrorismo, se puede llegar a presentar entre países que lanzan ataques cibernéticos a otros, de tal forma se han presentado esta clase de incidentes lo que ha provocado la caída de sitios web de entidades gubernamentales.

Aunque generalmente los países no aceptan que se están presentado este tipo de guerra cibernética.

Sería una estupidez desaprovechar las ventajas de un escenario de batalla tan fácil de usar por los gobiernos o ejércitos, es mucho más barato enviar un exploit o un troyano que un ejército, con todo el mantenimiento que supone material y humano. Además, bien hecho, puede ser el comando más indetectable de todos, por lo que todo son ventajas en un principio. [5]

III. BRECHAS DE SEGURIDAD

La puerta de entrada principal a las empresas para realizar ataques a la seguridad informática son las vulnerabilidades que tienen los sistemas, lo cual se denomina como brecha de seguridad.

Dentro de los ataques que se ha realizado recientemente es a “Adobe, comprometiendo 150 millones de cuentas, evento del cual se generaron otra serie de ataques como efecto dominó, donde estuvo comprometida la información de los usuarios.” [3]

Por esta razón es importante mantener actualizados los aplicativos, que para el caso de Adobe crea cambios que permiten mitigar o eliminar esta clase de inconvenientes, que afectan directamente al usuario y empresas.

Además es de vital importancia que las empresas tengan estipulado en su gestión de riesgos las posibles soluciones a pérdidas de datos, ocurrencia de desastres naturales, daño en la infraestructura tecnológica existente, seguridad a sistema de backups.

IV. LA LEY FRENTE A DELITOS INFORMÁTICOS Y DATOS PERSONALES

Como van siendo cambiantes las formas de hacer ciberdelicuencia, la ley debe estar al tanto para que se establezcan regulaciones y controles hacia los ataques a la seguridad informática.

Así los organismos de seguridad deben buscar tener control adecuado sobre este tipo de ataques y de la forma de hacer delito, para el caso de Colombia se deben crear unidades especiales encargadas de manejar las situaciones que se lleguen a presentar sobre la seguridad informática, ya que hace parte del día a día de las empresas y posiblemente de los hogares.

En Colombia hasta hace poco tiempo se crea una ley que hace que se establezcan controles y disposiciones hacia el manejo de la información que es suministrada a empresas de cualquier tipo, que son almacenadas en bases de datos propias, lo que puede llegar a ser un posible riesgos a ser

manipulada de forma indebida.

Se busca tener control sobre los datos personales que son suministrados, permitiendo a través de la ley Estatutaria 158 de 2012, de la república De Colombia, la cual dentro del Artículo 1, "tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías" [6]

Esta ley es aplicable en el país o en caso que la ley nacional pueda ser aplicada, por normas y tratados internacionales que así lo permitan.

De tal forma que no es aplicable en los siguientes casos:

A. Base de datos personal

Este tipo de base de datos solo es manipulada por la misma persona dueña de la información o personas allegadas.

B. Base de datos de seguridad o defensa nacional

Controlan la información de las personas que han sido involucradas en lavado de activos y control del terrorismo.

C. Bases de datos de inteligencia o contrainteligencia

La información es usada para fines netamente de la ley.

D. Base de datos periodístico

Tiene como fin el manejo de la información para llevar a cabo investigaciones dentro del periodismo

V. FALTA DE CONCIENCIA HACIA LOS ATAQUES DE SEGURIDAD INFORMÁTICA

Cada vez más se van hacer conocer a las personas sobre los tipos de ataques y los controles básicos que se deben llevar a cabo, haciendo de esto una rutina, de tal forma que en algún momento dado no va a ser de mayor importancia para las personas conocer más y controlar su información frente a este tipo de ataques.

Esto hace que se convierta en un posible problema, pues no va a existir la suficiente concientización que lleve a un nivel de autoprotección adecuada.

Las empresas por lo tanto deben instituir y realizar constantemente dentro de su programa de gobierno de la seguridad informática, métodos que muestren a su recurso humano los cambios y las consecuencias que pueden llegar a darse si no se tiene un adecuado manejo de la información.

Concientización del personal y a las personas que hacen parte de la organización es clave para buscar la protección y seguridad de la información, dando a conocer las consecuencias a las cuales están expuestos si son blancos de ataque, ya sea de tipo pasivo o activo.

Por lo tanto se debe dar a conocer a las personas la forma óptima del manejo de información en las redes sociales y en general en la web, pues se han llegado a conocer casos en los cuales con esta información el usuario puede llegar a ser un blanco por parte de personas inescrupulosas que buscan obtener información privilegiada, sin que sea evidente para la víctima.

VI. GESTIÓN Y MANEJO DE LOS DATOS

Es indispensable que si se debe realizar algún tipo de manipulación de datos personales en las empresas, se informe al dueño de la información sobre el manejo que se la van a dar a sus datos, para que a su vez exprese su autorización. Garantizando la posterior consulta de los cambios que haya sido realizados a sus datos.

Las empresas deben definir una serie de mecanismos para el correcto tratamiento de los datos personales. Al recolectar y manipular la información suministrada por los ciudadanos, deben cumplir y establecer mecanismos que permitan su manipulación de forma adecuada y cumpliendo a cabalidad con la ley estatutaria 1581 De 2012, que actualmente se rigen.

El Aviso de privacidad, es procedimiento para obtener la autorización del titular previo al inicio del tratamiento, Herramientas que garanticen condiciones de seguridad adecuadas para evitar la adulteración, pérdida, consulta, uso o acceso fraudulento sobre la información, Medidas tecnológicas para proteger los datos personales y sensibles, Manual interno de políticas y procedimientos para cumplir con la Ley sobre protección de datos, Elaborar las políticas del tratamiento de la información y suministrarlas al registro nacional de bases de datos, el cual está a cargo de la Superintendencia de Industria y Comercio. [7]

Según el artículo 10 de la ley la ley Estatutaria 158 de 2012, en los casos en los cuales no es necesaria la autorización de la persona dueña de la información es en los casos:

A. Información requerida por entidad pública o administrativa

Se requiere la manipulación de la información por orden judicial.

B. Datos públicos

Su naturaleza permite que sea manejada sin ningún inconveniente, pues se soporta que son de esta naturaleza.

C. Urgencia médica o sanitaria

Esta información es manejada por el personal de una entidad prestadora de servicios de salud, para determinar los datos más importantes que permitan establecer datos vitales que en un momento dado permitirá salvar la vida.

D. Autorizado para fines históricos

Los datos serán manipulados desde lo permitido en esta ley, con el fin de ser estudiado y referenciado desde el punto de vista histórico, científico o estadístico.

E. Registro civil de las personas

Ante el estado Colombiano, los ciudadanos deben ser registrados, para de esta forma sea asignado el número único de Identificación (NUIP), que le permite identificarse ante los demás ciudadanos, sin que haya lugar a repeticiones en la identificación como ciudadano Colombiano.

VII. IMPORTANCIA DE LA PRIVACIDAD DE LOS DATOS PERSONALES

En el congreso de Colombia se llevó a cabo un debate entre la superintendencia El senador Velasco argumenta que solo debe ser la autorización expresa e informada para la recolección de datos, y que no se debe permitir en Colombia la recolección de datos de forma tácita, (ejemplo, se me informó por correo que estoy en la base de datos de una empresa, NO respondo, la empresa continua usando mis datos). Estamos en un mundo conectado, pero los colombianos debemos tener en cuenta, que la privacidad es algo que no se puede dejar a un lado. [8]

De esta forma los ciudadanos debemos tener muy presente que todas las compañías deben cumplir con políticas de manejo de datos, de tal forma que las personas puedan acceder a los datos suministrados para comprobar su veracidad y de la misma forma poder realizar cambios en cualquier momento que se requiera.

VIII. PROGRAMA PARA PROTEGER LAS EMPRESAS DE CIBERATAQUES

Los gobiernos cada vez más están interesados en establecer medidas que permitan a las empresas dar un manejo óptimo y adecuado a los diferentes tipos de ataques cibernéticos.

De esta forma el gobierno de Estados Unidos en el mes de Febrero de 2014 presenta un proyecto que busca brindar apoyo a las empresas hacia este tipo de ataques.

La Casa Blanca ha presentado este miércoles la Red de Ciberseguridad, un proyecto cuyo objetivo es ayudar a las empresas estadounidenses a reducir los riesgos de ataques informáticos y mejorar la protección de sus infraestructuras. La iniciativa se enmarca dentro de la orden ejecutiva que el presidente Barack Obama firmó hace un año para responder a la amenaza cibernética. "Este programa está dedicado a ayudar a las compañías, a todas ellas, no importa su grado de sofisticación o su tamaño y está diseñado desde la perspectiva de las empresas no desde la del Gobierno", ha señalado la secretaria de Comercio, Penny Pritzker durante la presentación de la red de ciberseguirdad, un proyecto en el que además de su departamento está involucrado el de Seguridad Nacional. [9]

IX. CONCLUSIONES

Ante el constante cambio de los tipos de ataques realizados por Hackers, con los cuales buscan robar y/o manipular la información de las empresas, se debe también buscar la forma más adecuada para manejar los incidentes de seguridad de la información.

Se convierte en una tarea trascendental e indispensable concientizar al personal de la empresa así como a las personas externas que pueden llegar a manipular información importante de la misma, sobre los tipos de ataques que existen y como van evolucionando, haciendo de este tipo de actividades una labor cíclica dentro del manejo de la seguridad de la información.

Las empresas deben saber que los controles tradicionales no siempre son los mejores, pues cada vez más se conocen formas de vulnerar la seguridad informática de las empresas aún con este tipo de controles.

Seguridad de la información debe ser implantada como una medida preventiva más no correctiva, pues de esta forma la empresa puede llegar a tener consecuencias desfavorables o hasta poder ser el fin de su operación.

La Información es el activo más importante para las compañías, pues contienen datos de un alto valor para la persona dueña de la información, por lo cual en Colombia se crea la Ley Estatutaria 1581 De 2012, Tratamiento de datos personales, que hace que se tenga un control sobre la información de los ciudadanos y su tratamiento.

Esta ley define la forma como pueden ser tratados los datos personales y como pueden las personas tener control sobre los mismos, así como dar una regulación a los procedimientos que pueden llevarse a cabo sobre estos.

REFERENCIAS

[1] Edgar Sandoval ,” Ingeniería Social: Corrompiendo la mente humana”, 04 de Mayo de 2011, Tomado de página web .seguridad cultura prevención para TI http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana#_ftn1

[2] MOLIST, Mercè; Ingeniería Social: Mentiras en la Red; http://ww2.grn.es/merce/2002/is.html

[3] *Nuevos retos en seguridad informática, www.seguratec.com.co*, 2014.

[4] Mateo Santos, “Las tendencias de seguridad informática para 2014”, Diciembre de 2013, Tomado de la página web de revista Enter

http://www.enter.co/especiales/enterprise/las-tendencias-de-seguridad-informatica-para-el-2014/

[5] L. Gutierrez, "Curso ciberseguridad y hacking ético", Sevilla: Punto rojo libros, 2014, pp. 34.

[6] *Ley estatutaria 1581 de 2012, Congreso de Colombia*, Artículo 1, 2012.

[7] Certicámara, ABC para proteger los datos personales, Ley 1581 de 2012 Decreto 1377 de 2013",2013.

[8] Germán Realpe Delgado, "La protección de datos personales se volvió importante en Colombia", Agosto 2013, Tomado de la página web de revista Enter http://www.enter.co/especiales/enterprise/la-privacidad-y-la-proteccion-de-datos-en-colombia/

[9] Eva Sainz, "EE UU crea una red de seguridad para proteger a las empresas de ciberataques, http://internacional.elpais.com/internacional/2014/02/12/actualidad/1392230992_753620.html, Washington, 12 Febrero de 2014

Ana Rocío Castro Páez
Ingeniera de sistemas y computación
Universidad Pedagógica y Tecnológica de Colombia
Ingeniera de soporte técnico
Departamento Administrativo de la presidencia de la república – DAPRE
Estudiante de especialización en seguridad informática
Universidad Piloto de Colombia
Junio de 2015